FOSI
Family Online Safety Institute

Ofcom Children's Code - FOSI Response

July 17, 2024

The Family Online Safety Institute (FOSI) would like to take this opportunity to respond to the recent consultation regarding the Children's Code. We appreciate the chance to contribute our insights and provide feedback on this matter. Our response reflects our commitment to children's safety and we hope to engage in a productive dialogue to achieve the best possible outcomes.

FOSI is an international, non-profit, membership organization working to make the online world a safer place for children and their families. We achieve this by identifying and promoting best practices, tools, and solutions in the field of online safety. FOSI convenes leaders in industry, government, academia, and the non-profit sectors to collaborate and innovate new solutions and policies that ensure a safer, more rewarding digital experience for all. Through research, resources, events, and special projects, FOSI promotes a culture of responsibility online and encourages a sense of digital citizenship for all.

FOSI defines online safety as *acknowledging the risks and mitigating the harms in order to reap the rewards of digital life*. We believe that online safety and data privacy are complementary parts to protecting young people online, and we are glad to see Ofcom and the ICO thoughtfully approach these issues as the UK seeks to become the safest place for a child to be online.

Thank you for considering our input.

Transatlantic Children's Online Safety and Privacy

While FOSI is based in Washington, D.C., the impacts of the Children's Code and subsequent guidance and regulation will be keenly felt across the Atlantic, if not around the globe. The United States still does not have a federal comprehensive data privacy law. Individual states have begun to pass their own data privacy laws, but they vary so significantly that now a patchwork of laws exists. An individual's rights and protections differ drastically depending on where they live, work, and travel throughout the country. This situation also creates a compliance nightmare for online platforms.

States have also tried to pass their own versions of online safety laws, modeled after the UK's Children's Code. These Age Appropriate Design Codes have already been effectively challenged in court, and California's law has been suspended while a lawsuit proceeds arguing that the law violates the First Amendment's protection of free speech.

While the US does not have a dedicated agency dedicated to online safety or privacy, the Federal Trade Commission (FTC) has overseen the regulation of the Children's Online Privacy Protection Act (COPPA) for over two decades. The FTC will take a keen interest in what guidance and regulation Ofcom produces, and learn from its regulatory cousin across the pond.

With a handful of efforts and new regulations in the US, though none of them at the federal level, the implementation of the UK's Children's Code has the potential to become a baseline standard for more than just the UK.

Age Assurance

Age Assurance is a critical component to online safety. In order to provide age appropriate experiences, platforms need to know (with varying degrees of certainty) how old a user is. While there is no silver bullet to easily keep all children safe online, improving age assurance processes and regulations can improve online safety.

In 2022, we conducted original research into age assurance that focused on parents and teens in the US, UK, and France. This research was then instrumental in informing our white paper on age assurance.

One of our takeaways from this work on age assurance is the important balance of invasiveness and effectiveness. That is, in order for an age assurance process to be more effective (a higher level of assurance), more data must be obtained from a user (more invasiveness). If a platform must know with 100% certainty that a user is over 18, then it would use an age assurance method that requires personal information such as a government ID or a credit card. On the other end of the spectrum, the lowest level of age assurance (such as a self declaration checkbox or birthdate entry) requires the least amount of personal information, and is therefore more privacy preserving, but less effective at ascertaining the age of the user.

A middleground exists between these two extremes, and includes a range of new age estimation technologies. Such technologies can use facial scans or voice analysis to estimate a user's age range within a certain level of confidence. Since some of these technologies rely on sensitive biometric data, age estimation methods present varying levels of accuracy and privacy. Age assurance processes present a delicate tradeoff that must be carefully considered by regulators.

Another takeaway expands on the invasiveness-effectiveness tradeoff, revealing the benefits of a risk-based, proportional system. This means that for the platforms, content, and online activities deemed least dangerous, a lower level of age assurance would be acceptable. Whereas the most dangerous online activities (such as purchasing a weapon, alcohol, or other controlled substance) could require the highest level of age assurance. There is a sliding scale here and it is difficult to ascribe level of risk, but addressing age assurance regulation from a risk-based and proportional approach can lead to an acceptable balance of invasiveness and effectiveness.

Safety by Design

While Ofcom has new and specific authority to regulate online safety in the UK, it does not have to start from scratch. There are other actors around the world that have been researching, experimenting with, and regulating safety by design. Notably, Australia's eSafety Commissioner has been working on online safety by design for the past six years, and has produced principles, research, and resources available online.

Additionally, the OECD recently released a new report on Digital Safety By Design for children. This report highlights actions and approaches that industry can take to design its products with the safety of the youngest users in mind, but also in a rights-respecting way that does not significantly limit or prevent children from being online. Ofcom would be wise to take these thoughtful recommendations into consideration.

While parental controls and user online safety tools can be effective in creating safer, customized online experiences for young people, they should not be the sole solution but instead must be part of a more comprehensive approach. In our research into parental controls and user online safety tools, we found that parents are overwhelmed by the amount of apps, platforms, and services that their children use, especially in searching for, learning about, and turning on safety settings for each app. Parental controls and online safety tools are most effective when they are a part of what we call the culture of responsibility: where platforms, policymakers, educators, and law enforcement all recognize and take responsibility for the roles they play in improving online safety. If platforms prioritize safety and privacy by default and by design, parental controls and online safety tools will be complementary protections for children and families instead of the only solution.

An overreliance on parental controls in the United States brings additional concern, as the US has not ratified the United Nations Convention on the Rights of the Child. The US does not consider children's rights in the same context as the rest of the world, and instead focuses on parents' rights to raise their children. Any regulation about parental controls must ensure that they do not overpower parents by offering full surveillance tools that would violate minors' rights to privacy and access to information.

Empowering young users and recognizing their agency is important, but children should not be solely responsible for protecting themselves online. Platforms should consider safety by design principles in their product development to not only protect children from seeing age inappropriate content but also to protect them from functionality which can expose them to harm, e.g. live streaming.

Industry Expectations

As mentioned above, this regulation has the potential to influence practices around the world. Many platforms and companies operate internationally and are looking for an effective standard to implement on a global scale. To that end, we would like to mention the work of the Global Online Safety Regulators Network. As FOSI is an observer of the Network and Ofcom is both a member and current chair, we know your deep familiarity of the Network and its work. We raise it here in order to stress the benefits of working to harmonize international approaches to online safety. As the Network itself iterates, the goal is not identical online safety laws in every country, but laws that take into account regional and local cultural differences, based on shared principles that are similar enough for compliance and enforcement to be harmonized across jurisdictions.

There are many regulatory regimes emerging across the world and it is important that each of the regimes seeks to support and work in sync with one another. FOSI industry members are keen to ensure that there is some synergy in order to better develop solutions to online harms. Without complimentary regulatory approaches, there are real compliance challenges for industry. There is an opportunity through this regulation to establish a strong baseline standard that other countries can find harmony with and that industry can comply with, therefore improving online safety globally.

Aspirations of the Code

The Children's Code has the potential to be a strong baseline safety standard that reaches across the entire world. The first of its kind regulation made significant impacts when it went into effect and became enforceable, with platforms improving default safety and privacy settings while continuing to innovate additional protections for minors. Through this regulation, the UK again has the chance to influence and improve online safety for all children and families.

We would like to see the Code ensure that platforms are aspirational about their child safety duties and that it is agile enough to cope with new challenges and risks. As technology changes at a rapid pace, it is important that platforms continue to evolve and advance their online safety work.

The risk assessments and the child access assessments outlined in the Code present opportunities for platforms to better protect children. Ofcom should ensure that the assessments that are produced are robust and actually better protect children. The assessments must result in meaningful changes to design and functionality and success must be observable.

Thank you for being thoughtful and deliberate in regulating online safety, especially for children and minors. We appreciate the opportunity to give input and thank you for your consideration.

Stephen Balkam
Founder and CEO, Family Online Safety Institute